UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/966,224	09/28/2001	Michael D. Ruehle	42390P11974	5894

8791 7590 03/29/2006

BLAKELY SOKOLOFF TAYLOR & ZAFMAN
12400 WILSHIRE BOULEVARD
SEVENTH FLOOR
LOS ANGELES, CA 90025-1030

EXAMINER	
COLIN, CARL G	
ART UNIT	**PAPER NUMBER**
2136	

DATE MAILED: 03/29/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/966,224	RUEHLE ET AL.	
	Examiner	Art Unit	
	Carl Colin	2136	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *13 January 2006*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-29* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-29* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *1/22/2002* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date *see att*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

Response to Arguments

1. In response to communications filed on 1/17/2006, the following claims 1-29 are presented for examination.

1.1 Applicant's remarks, pages 8-9, filed on 1/17/2006, with respect to the rejection of claims 1-29 have been fully considered but they are not persuasive. With respect to the double patenting rejection, as referred in the MPEP by Applicant, claims may be differently worded and still define the same invention. Applicant states, "the specification (par 30-31) describes a modular exponentiator which includes a modular multiplier. Applicants note that modular exponentiator and a modular multiplier are not equivalent. Seeing that a modular exponentiator as described includes a modular multiplier, the present application is distinct from the reference", Applicant's arguments above do not comply with 37 CFR 1.111(c) because they do not clearly point out the patentable novelty which he or she thinks the claims present in view of the state of the art disclosed by the references cited or the objections made. Further, they do not show how the claim limitations avoid such references or objections. In addition, the general allegation made by Applicant is not sufficient evidence that the claims do not define the same invention. Applicant's statement is even a contradiction of the specification that also recites "modular exponentiator includes a first modular exponentiator..." In response to applicant's argument that the references fail to show certain features of applicant's invention, it is noted that the features upon which applicant relies (i.e., a modular exponentiator that includes a modular multiplier) are

not recited in the rejected claim(s). Although the claims are interpreted in light of the specification, limitations from the specification are not read into the claims. See *In re Van Geuns*, 988 F.2d 1181, 26 USPQ2d 1057 (Fed. Cir. 1993). It is also noted that the claims are differently worded to replace independent communication channels of the reference with modular exponentiator not the term multiplier as argued by Applicant above.

With respect to the 103 rejection of claims 1-29, Applicant's arguments fail to comply with 37 CFR 1.111(b) because they amount to a general allegation that the claims define a patentable invention without specifically pointing out how the language of the claims patentably distinguishes them from the references. As discussed above, Applicant's argument that the reference does not disclose "exponentiators" is not persuasive. Examiner asserts that the claim limitations are rejected as claimed. Applicant's statement that the Office Action asserts on page 3 (that multiplier units 28a and 28b disclose multiple exponentiators) is erroneous. Examiner cannot find this citation on page 3 of the last Office Action. It remains the examiner's position that claims 1-29 are still rejected for at least the reasons cited above.

Double Patenting

2. A rejection based on double patenting of the "same invention" type finds its support in the language of 35 U.S.C. 101 which states that "whoever invents or discovers any new and useful process ... may obtain a patent therefor ..." (Emphasis added). Thus, the term "same invention," in this context, means an invention drawn to identical subject matter. See *Miller v. Eagle Mfg. Co.*, 151 U.S. 186 (1894); *In re Ockert*, 245 F.2d 467, 114 USPQ 330 (CCPA 1957); and *In re Vogel*, 422 F.2d 438, 164 USPQ 619 (CCPA 1970).

A statutory type (35 U.S.C. 101) double patenting rejection can be overcome by canceling or amending the conflicting claims so they are no longer coextensive in scope. The filing of a terminal disclaimer cannot overcome a double patenting rejection based upon 35 U.S.C. 101.

2.1 Claims 1, 2, 17, 9, 16, 21, 22, 24, 25, and 27 and the intervening claims are rejected under 35 U.S.C. 101 as claiming the same invention as that of claims 1, 3-5, 9-13 13, 16, 19, 21-24, 26, 30, and 33 of prior U.S. Patent No. 6,922,717. This is a double patenting rejection.

Claim Rejections - 35 USC § 103

3. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

3.1 **Claims 1-29** are rejected under 35 U.S.C. 103(a) as being unpatentable over US Patent 6,240,436 to **McGregor** in view of US Patent 5,189,636 to **Patti et al** *(Applicant's Disclosure)*.

3.2 **As per claims 1-3, 9-11, 16-18, 21-23, and 24-29, McGregor** substantially teaches method apparatus, and system comprising; a memory (ROM RAM) to store data and instructions (see figure 1 with detailed explanation); a first processor (CPU) coupled to said memory to process data and execute instructions (see figure 1 with detailed explanation); and a second processor (20) coupled to said memory, said second processor comprising: a plurality of modular exponentiators (28) including a first modular exponentiator and a second modular exponentiator (see figure 2 with detailed explanation), and a coupling device (22) interposed between said first modular exponentiator and said second modular exponentiator to receive a control signal (column 4, lines 23-25) and said apparatus or system having a first mode of operation corresponding to a first state of said control signal wherein said first modular exponentiator is operably separated from said second modular exponentiator (see column 4, line 39 through column 5, line 65). **McGregor** also suggests that processor size can be selected to suit operand size to reduce the number of required computations (column 2, lines 30-34). **McGregor** does not explicitly teach receiving a control signal to selectively couple said first modular exponentiator to said second modular exponentiator in response to a state of said control signal. **Patti et al** in an analogous art teaches a method, apparatus, system, and processor of a dual mode combining circuit which can be conditioned by a mode control signal to operate either as two n-bit adders in a first mode of operation corresponding to a first state of a control signal or to operate as a single 2n-bit adder in a second mode of operation corresponding to a second state of said control signal, where n is an integer (see abstract and claim 1, column 63, lines 4-35). Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to combine the dual mode of operation of **Patti et al**

to the teaching of high speed computation of modular exponentiations of **McGregor** to provide a dual mode operation to selectively separate or couple the modular exponentiators or multipliers of **McGregor** according to a first and second state of operation respectively as taught by **Patti et al**. One skilled in the art would have been lead to make such a modification because by selecting the appropriate multiplier size according to operand size, an increase in speed and performance would be provided as suggested by **McGregor** (column 2, lines 30-34 and 39-45) and **Patti et al** (see abstract).

As per claims 4, 12, and 19, McGregor suggests computation of exponentiation of 1024 2n bits that meets the recitation of wherein n equals 512 (column 1, lines 55-65 and column 4, lines 38-53 and column 2, lines 39-45). Using different size of modular exponentiators would have been an obvious modification as it is known in the art and would not depart from the spirit and scope of the references as combined above.

As per claims 5-6, and 13, McGregor discloses the limitation of wherein each of said plurality of modular exponentiators comprises a modular multiplier to perform a modular multiplication of the form A x B mod M, where A, B, and M are all integers (column 5, line 30 through column 6, line 18).

As per claims 7 and 14, McGregor discloses the limitation of wherein said modular multiplier comprises a systolic array of processing elements (column 3, line 50 through column 4, line 7).

As per claims 8, 15, and 20, Patti et al discloses the limitation of wherein said a coupling device comprises a multiplexer (column 7, lines 29-53). Therefore, claims 8, 15, and 20 are rejected on the same rationale as the rejection of claims 1, 9, and 16 above.

Conclusion

4. **THIS ACTION IS MADE FINAL.** Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

4.1 The prior art made of record and not relied upon is considered pertinent to applicant's disclosure as the art discloses multipliers or adders that support multiple numbers with different bit lengths and co-processor for increasing speed in performing modular exponentiation.

US Patents: 5,327,369 Ashkenazi ; 5,943,250 Kim et al ; 6,237,016 Fisher et al ; 6,209,016 Hobson et al ; 6,434,585 McGregor.

4.2 Any inquiry concerning this communication or earlier communications from the examiner should be directed to Carl Colin whose telephone number is 571-272-3862. The examiner can normally be reached on Monday through Thursday, 8:00-6:30 PM.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on 571-272-3795. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

cc

Carl Colin
Patent Examiner
September 18, 2005

CHRISTOPHER REVAK
PRIMARY EXAMINER

CR 3/26/06